

Cazador cazado

by javier - Miércoles, julio 22, 2015

<http://memoriasdeunsysadmin.tk/2015/07/22/cazador-cazado/>

Esta es una más que agradable noticia para mi, debo decirlo. Hacking team es una compañía que se dedica a la seguridad informática(o debiera decir mejor, a la INseguridad), ya que se especializa en desarrollo de soluciones de intrusión, vigilancia, control remoto, etc, para proveer a gobiernos de todo el mundo.

El asunto es que esta vez les tocó a ellos, ya que sus sistemas fueron comprometidos y se liberaron y subieron a torrent 400GB de código fuente, comunicaciones por email y documentación interna. Los atacantes además lograron acceder al twitter de la empresa, donde subieron imágenes de la información obtenida, como así también alteraron su biografía y publicaron mensajes.

A pesar de que la firma se apuró a destacar en su sitio, que dichos datos son ya viejos y desactualizados, los documentos incluyen al parecer, mails con contactos de diversos gobiernos que revelaría servicios y facturas a países de todas las latitudes. De momento se sabe, basado en la fuga de información, de clientes en Egipto, Etiopía, Nigeria, Chile, México, Mongolia, Corea del Sur, Vietnam, Australia, Alemania, Italia, Suiza, España, Arabia Saudita, entre tantos otros.

La documentación también sirvió para confirmar sospechas negadas por Hacking Team, acerca de negocios con Sudán y demás gobiernos opresores, lo cual viola su supuesta observación de la declaración de los derechos humanos.

A medida que el torrent en cuestión comenzó a circular, el daño fue cada vez mayor para la firma italiana, saliendo a la luz entre otras cosas:

Facturación a los distintos clientes, algunos ejemplos: Contrato por 3.4 millones de euros con el Centro Nacional de inteligencia de España, con vigencia hasta enero del 2016; pago de 480 mil euros con la Natioanl Intelligence ans Security Services, de Sudán; pago de 1 millón de birres(moneda de etiopía) del gobierno Etíope por el sistema de control remoto, servicios profesionales y equipamiento de comunicaciones; etc



Contrato con Etiopía



Contrato con Sudán

Detalles de vigencias de contrato con sus clientes, que incluye algunos, como Rusia y Sudán con un lindo cartel "No soportado oficialmente"

ALFAHAD-PROD	Morocco	Minister of Interior	11/31/2014	Active
CSDN-01	Morocco	Intelligence Agency	11/31/2014	Active
BGGO	Nigeria	Bayelsa Government	11/31/2013	Expired
ORF	Oman	Excellence Tech group Oman	11/31/2014	Active
PANP	Panama	President Security Office	5/31/2014	Expired
KWANT	Russia	Intelligence Kvant Research	11/31/2014	Not officially supported
GP	Saudi Arabia	General Intelligence Presidency	11/31/2015	Active
MCD	Saudi Arabia	Minister of Defence	7/31/2015	Active
TCC-04D	Saudi Arabia	General Intelligence Directorate	6/31/2015	Active
IDA-PROD	Singapore	Infocomm Development Agency	3/31/2015	Active
SKA	South Korea	The Army South Korea	11/31/2014	Active
NSS-01	Sudan	National Intelligence Security Service	11/31/2014	Not officially supported
THDOC	Thailand	Thai Police - Dep. Of Correction	7/31/2014	Expired
ATI	Tunisia	Tunisia (demol)	3/31/2011	Expired
TRP	Turkey	Turkish Police	11/31/2014	Active
MCI	UAE	Minister of Interior	11/31/2014	Active

Fragmento de su lista de clientes y status.

Contraseñas de personal de Hacking Team: Uno de los más afectados sin duda, fue uno de sus Ingenieros

de Seguridad, cuyas contraseñas de redes sociales, paypal, dispositivos de red e incluso bancarias, vieron la luz.

Contraseñas de sus clientes, mostrando el uso de contraseñas bastante débiles y cortas en la mayoría de los casos.

Al parecer, Hacking Team no se ha rendido sino que más bien desmiente fuertemente que los datos publicados sean vigentes, cómo así también expresa que se ha hecho la denuncia pertinente al gobierno para buscar a los responsables del "delito". Hay que decirlo también, nadie nunca está suficientemente preparado para un golpe así, ni siquiera las empresas más grandes de seguridad. La posibilidad siempre está y el peor error es pensar que a uno no le va a pasar. A usar contraseñas fuertes! Y en lo posible, encripten sus documentos importantes también.

Saludos,

memoriasdeunsysadmin.tk